УДК 681.3

О.Г. СТАРУСЕВ, канд. техн. наук, НТУ "ХПИ" (г. Харьков)

ФОРМАЛЬНОЕ ОПИСАНИЕ ФУНКЦИОНИРОВАНИЯ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ

У статті наведено огляд проблеми формальної специфікації та верифікації мережевих протоколів, розглянуто опис протоколу АВР із допомогою ряду автоматних формальних методів та наведено ряд міркувань з верифікації мережевих протоколів.

In this article, the survey of network protocols formal specification and verification problem was considered. The description of protocol ABP through state charts and pseudo-formal specifications was considered. Also, are resulted some considering of protocols verification.

Постановка проблемы. Интенсивное использование распределенных вычислительных систем и сетей передачи данных в промышленности и бизнесе накладывает дополнительные требования по надежности и эффективности методов проектирования и реализации протоколов и систем передачи данных.

Одним из основных требований к описанию протоколов является соответствие их стандартам Международной организации по стандартизации (МОС или ISO) [1] в рамках эталонных моделей.

Для формального описания протоколов может использоваться два класса формальных методов – конечно-автоматные (КА) и алгебраические методы. При описании эталонной модели OSI (Open System Interconnection) используются оба вида методов. Так формальный метод Estelle [2] относится к классу конечно-автоматных методов, а метод LOTOS [3] – к классу алгебраических методов. При этом метод Estelle используется для описания протокольных стандартов, а метод LOTOS – для описания стандартов сервиса, предоставляемого протоколами.

Основными критериями при использовании того или иного формального метода являются применимость, степень абстракции, описательная мощность и анализируемость [4].

Приведенные методы формального описания и верификации реализованы в виде инструментальных комплексов и позволяют создавать протоколы в виде формальных спецификаций с последующей трансляцией полученных формальных спецификаций в реализации на языках высокого уровня (например, языки C, C++ или Java).

Анализ литературы. В настоящее время опубликован большой объем литературы, посвященный методам формального описания протоколов. Кроме рекомендованных МОС методов Estelle и LOTOS, существует много других методов, которые относятся к этим двум классам. К алгебраическим методам

относятся алгебры взаимодействующих процессов (ACP [5], CSP[6], CCS [7]), методы на временной логике [8], метод трассовых спецификаций [9] и т.д. Ко второму классу относится группа КА методов, включающая в себя использование расширенных КА. Это такие методы, как сети Петри [10], диаграммы состояний и соответствующие формальные методы (Estelle, Esterel [11], Unity [12], SDL [13] и т.д.).

Цель статьи. Целью этой статьи является рассмотрение методов спецификации сетевых протоколов на примере протокола ABP.

Формальное описание функционирования протоколов. В качестве объекта исследований был выбран один из простых протоколов – т.н. «протокол с нумерацией по модулю два» (Alternating Bit Protocol) [14]. Согласно модели OSI этот протокол относится к канальному уровню и обеспечивает гарантированную передачу данных через среду передачи с помехами. Предполагается, что среда передает пользователю пакеты, а пользователи верхнего (сетевого) уровня – пакеты.

Общие принципы функционирования протокола ABP следующие: 1) сообщение передается в отведенное время; 2) отправленное сообщение может быть получено или потеряно; 3) если сообщение получено, то отправляется подтверждение; 4) подтверждение может быть принято или потеряно; 5) если подтверждение не получено за заданное время, то сообщение отправляется повторно и т.д. Это гарантирует доставку сообщения.

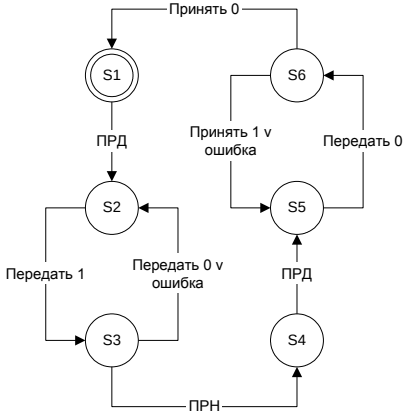

Рис. 1. Протокольный автомат передатчика

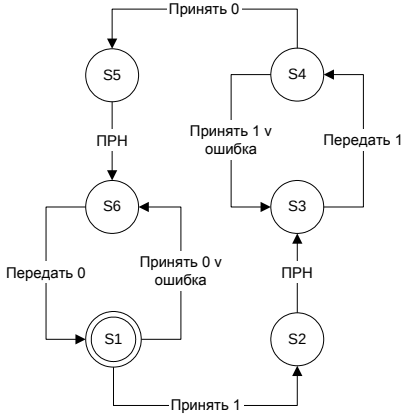

Рис. 2. Протокольный автомат приемника

Как видно из описанного выше алгоритма среда может задержать или исказить передаваемый пакет. Модель среды передачи можно представить в виде синхронного КА, где синхронность обозначает, что сообщения

принимаются и передаются в каждый интервал времени. Если сообщений нет, то передаются и принимаются пустые сообщения.

Автоматная спецификация протокольных объектов «передатчик» и «приемник» приведена на рис. 1 и 2. Описание работы автоматов представлено в виде диаграмм состояний. Функционирование протокольных объектов можно представить и в виде программ, близких к Estelle-спецификациям. Эти спецификации приведены на рис. 3 и 4. Полный протокольный автомат без учета тайм-аутов приведен на рис. 5.

```
Specification ABP_Transmitter;
type
 дан_тип = array[1..1024] of char;
var
  неподтв : пакет;
  переданный : пакет(0,1);
  данные : дан_тип;
  номер_птв : set(0,1,Error);
  a,d, x : дан_тип;
begin
  неподтв := 1; переданный := 0;
  loop
  if переданный <> неподтв then
   ПРД;
   переданный := переданный ⊕ 1;
   данные := x; fi
  a := [переданный, данные];
  передать; принять;
  номер_птв := d;
  if номер_птв = неподтв then
   неподтв := неподтв ⊕ 1;
 endloop
end
```

Рис. 3. Спецификация протокольного объекта «Передатчик»

```
Specification ABP_Receiver;
type
 дан_тип = array[1..1024] of char;
var
  ожидаемый : пакет(0,1);
  данные : дан_тип;
  номер_пкт : set(0,1,Error);
  b,g, y : дан_тип;
begin
  ожидаемый := 1;
  loop
    принять;
    [номер_пкт, данные] := b;
  if номер_пкт <> ожидаемый then
   передать_данные_польз;
   y := данные;
   ПРН;
   ожидаемый := ожидаемый ⊕ 1; fi
  b := ожидаемый;
  передать;
 endloop
end
```

Рис. 4. Спецификация протокольного объекта «Приемник»

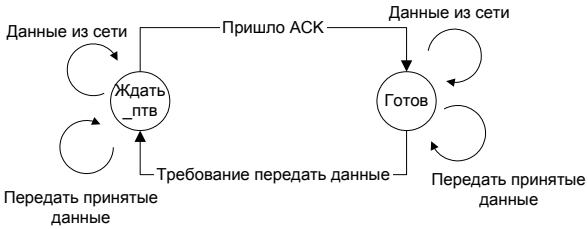

Рис. 5. Конечный автомат для протокола АВР

Необходимо отдельно остановиться на анализируемости КА методов. Для полученных спецификаций используются различные виды анализа достижимых состояний и доказательства инвариантных утверждений. Анализ достижимых состояний легко поддается автоматизации, но в связи с большими

размерностями требует применения дополнительных методов декомпозиции, редукции, ограничений рассматриваемых ситуаций и т.д. Доказательство инвариантности утверждений носит для этой группы «ручной» характер и требует высокой квалификации разработчика. Хотя с развитием систем логического вывода появляется возможность автоматизации процесса доказательства корректности.

Для формальной верификации важно то, что модель КА точно транслируется в спецификацию и наоборот. Наиболее распространенными проблемами для КА методов являются неограниченный рост числа событий (в нашем случае – неограниченный рост числа событий в канале между сервисным и протокольным автоматом) и возникновение ситуации непредусмотренного приема. При этом в реализации необходимо будет предусмотреть выдачу нескольких запросов на один фрейм данных.

Выводы. Основными преимуществами использования КА методов формального описания протоколов являются низкая степень абстракции. Эти методы хорошо изучены, хорошо подходят для описания протокольных объектов и их реализации. К сожалению, эти методы подвержены ряду недостатков, таких как быстрый рост числа состояний и ограниченные возможности формальной верификации. В дальнейшем необходимо специфицировать протокол при помощи алгебраических методов (LOTOS, CSP или OBJ [15]) и провести сравнение полученных результатов для определения наиболее эффективного способа спецификации сетевых протоколов.

Список литературы: **1.** *Международная организация по стандартизации и сертификации* http://www.iso.ch. **2.** *Turner K.J.* Using formal description techniques. – An Introduction to Estelle, Lotos and SDL. – John Wiley & Sons, 1993. – 431 p. **3.** *Van Eijk P.H.J. et al.* The formal description technique LOTOS. – North-Holland: Elsevier, 1989. – 453 p. **4**. *Зайцев С.С.* Описание и реализация протоколов сетей ЭВМ. – М.: Наука, 1989. – 272 с. **5.** *Bergstra A., Klop W.* Algebra of communicating processes with abstraction // Journal of Theor. Comp. Science. – 1985. – № 37 (1). – P. 77–121. **6.** *Хоар Ч.А.* Взаимодействующие последовательные процессы. – М.: Мир, 1989. – 264 с. **7.** *Milner R. A.* Calculus of Communicating Systems. – LNCS. – Vol. 92. – Springer, 1980. – 140 p. **8.** *Manna Z., Pnuelli A.* The Temporal Logic of Reactive and Concurrent Systems.– NY: Springer, 1991. – 226 p. **9.** *Bojanowski, J. et al.* Functional Approach to Protocols Specification // Protocol Specification, Testing and Verification XIV, Vuong, S.T., Chanson, S.T. (Eds.), Chapman & Hall, 1995. – P. 395–402. **10.** *Питерсон Дж.* Теория сетей Петри и моделирование систем. – М.: Мир, 1984. – 284 с. **11.** *Halbwachs N.* Synchronous Programming pf Reactive Systems. – Kluwer Academic Pub., 1993. – 184 p. **12.** *Misra J., Chandy K.M.* Parallel Program design – Addison-Wesley, 1988. – 325 p. **13.** *Doldi L.* Validation of Communications System with SDL: The Art of SDL Simulation and Reachability Analysis. – John Wiley & Sons, 2003. – 310 p. **14.** *Bartlett K.A., Scantlebury R.A., Wilkinson P. T.* A note on reliable full-duplex transmission over half-duplex links // Comm. ACM. – 1969. – Vol. 12. – № 5. – P. 260–261. **15.** *Goguen J., Malcolm G.* Software Engineering with OBJ: algebraic specification in action. – Kluwer Academic Pub., Boston, 2000.

Поступила в редакцию 11.04.2005